UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/614,983	07/12/2000	John R. Hind	5577-204	2458

20792 7590 01/27/2005

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
ADAMS, JONATHAN R	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/614,983	HIND ET AL.	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to applicant's arguments stating that Davis does not teach the use of update rules, as broadly as stated in the claims, the digital signature validity check and revision date validity check (Col 4, Line 11, '986) constitute update rules. Starting on Col 4, Line 1, Davis teaches "using the well-known techniques of digital signatures and certificates to validate the integrity and validity of the 'new BIOS program'". Davis further teaches on Col 4, Line 13, "If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and is never used."

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-60 rejected under 35 U.S.C. 102(b) as being preceded by Davis, US Patent NO. 5844986(hereafter referred to as '986).

3. As to claims 1 and 21:

'986 teaches a method for providing secure BIOS firmware updates comprising:

Obtaining an update image corresponding to the update of the programmable memory / Cryptographic coprocessor either passively/actively receives the new BIO program code (Col 3, Line 55, '986)

Obtaining/evaluating application rules information from certificate associated with update / Digital signatures used in BIOS upgrade software (Col 4, Line 27, '986), Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986)

4. As to claims 2 and 22:

Update application rules comprise at least one of rules information associated with a manufacturer of a device... / Certificate associated with manufacturer (Col 2, Line 49, '986)

5. As to claims 3, 4, 23, and 24:

Update application rules comprise rules defining devices for which application of the update image is authorized... authorized device manufacturers / Certificate associated with manufacturer (Col 2, Line 49, '986)

6. As to claims 5 and 25:

Update application rules comprise rules defining how data form update iage is utilized to update programmable memory / If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and never used (Col 4, Line 13, '986)

7. As to claims 6 and 26:

Update application rules comprise rules which identify installation information provided with the update image, utilizing the installation information / Digital signatures used in BIOS upgrade software (Col 4, Line 27, '986), Cryptographic coprocessor makes a validity determination based on the new BIOS program (Col 4, Line 8, '986)

8. As to claims 7 and 27:

'986 teaches a method for providing secure BIOS firmware updates. '986 does not specifically teach for the BIOS management utility software to be obtained via download. The examiner takes official notice as to obtain the BIOS management utility software with BIOS upgrade via download. It would have been obvious to a person of ordinary skill in the art at the time of invention to obtain the BIOS management utility software with BIOS upgrade via download. One of ordinary skill in the art would have been motivated to obtain the BIOS management utility software with BIOS upgrade via download because it is customary to make Internet upgrades available with an installation program. Examples include Microsoft Windows upgrades and peripheral device driver upgrades, etc.

9. As to claims 8 and 28:

Verifying the authenticity of the update / Cryptographic coprocessor performs the appropriate authentication operations on the new BIOS program (Col. 3, Line 61, '986)

10. As to claims 9 and 29:

Evaluating the certificate... valid digital signature / Using the well known techniques of digital signatures and certificates to validate the integrity and validity of the new BIOS program (Col. 4, Line 1, '986)

11. As to claims 10 and 30:

Decrypt the digital signature using a shared secret / authentication can be preformed... by the use of secret information (Col. 3, Line 65, '986)

12. As to claims 11 and 31:

Decrypting a digital signature using a public key from a certificate authority... comparing with precomputed value / public/private key cryptography... using techniques of digital signatures (Col. 3, Line 67, '986)

13. As to claims 12 and 32:

Public key is stored in non-updateable memory / Cryptographic coprocessor will be preloaded with the public key (Col 4, Line 31, '986)

14. As to claims 13 and 33:

Provide public key in previous version... obtain public key from programmable memory / Cryptographic coprocessor may be preloaded with another public key that may be used

to authenticate a certificate chain to obtain this industry association public key (Col 4, Line 34 et seq., '986)

15. As to claimss 14, 15, 34, and 35:

Hierarchical plurality of certificates / certificate chain (Col 4, Line 36, '986)

16. As to claims 16 and 36:

Hierarchical plurality of certificates / certificate chain (Col 4, Line 36, '986)
Extract update application rules from each of the certificates / Using the well known techniques of digital signatures and certificates to validate the integrity and validity of the new BIOS program (Col. 4, Line 1, '986)

17. As to claims 17, 20, 37, and 40:

Update only if all update application rules indicate that the update image is applicable to the device / Cryptographic coprocessor makes a determination as to the validity of the new BIOS program... revision date may be inappropriate ... If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and never used (Col 4, Line 13, '986)

18. As to claims 18, 19, 38, and 39:

Update if any update application rules indicate that the update image is applicable to the device / In an authentication using only one application rule such as the validity of a digital signature, any of the [one] rules would render the update image applicable

19. As to claims 41-60:

Claims 41-60 correspond to claims 1-20.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

21. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is

(571)272-3832. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (571)272-3838. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100